

ETHAN DARNELL, on behalf of himself and all others similarly situated,	)	Case No.: _____
	)	
	)	
Plaintiff,	)	
	)	
v.	)	<u>DEMAND FOR JURY TRIAL</u>
	)	
WYNDHAM CAPITAL MORTGAGE, INC.,	)	
	)	
	)	
Defendant.	)	
	)	
	)	

Plaintiff Ethan Darnell (“Plaintiff”) brings this Class Action Complaint against Wyndham Capital Mortgage, Inc. (“Wyndham” or “Defendant”) as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsel’s investigations, and upon information and belief as to all other matters, as follows:

1. Wyndham is a nationwide mortgage provider and refinancee that claims to have funded over \$18 billion in loans for over 60,000 clients. The privately held corporation states that it uses “advanced technology” for its strictly online loan processes in an effort to streamline the loan process. In late 2019, Wyndham announced a “rapid expansion” of its sales and operation teams due to increased demand. Wyndham has seen an incredible increase in business in 2020, with more than double the number of funded loans compared to 2019.

2. Beginning on or about October 2020, Wyndham notified various states' Attorneys General and thousands of current and former clients about data breaches that occurred through Wyndham's email services. First, on October 16, 2020, Wyndham warned that on September 18, 2020, an email was sent "in error" by a Wyndham employee to an email account not belonging to

Wyndham or its authorized affiliates.<sup>1</sup> The information included in the email contained clients' sensitive personal information, including but not limited to clients' names, Social Security numbers, email addresses and "loan data" ("PII"). The "loan data" was extensive in that it included information supplied by clients to Wyndham to secure a mortgage. Second, on or about October 23, 2020, Wyndham warned that it discovered that an employee was the "victim of a phishing scam" that compromised Wyndham's security protocols and allowed unauthorized third parties access to the employee's email account for an extensive period; from June 30, 2020 through August 3, 2020<sup>2</sup> (collectively, "Data Breaches").

3. The Data Breaches allowed criminals to obtain everything they needed to illegally use Wyndham's current and former clients' PII to steal their identities, make fraudulent purchases, and to commit myriad financial crimes and fraud.

4. Not only did hackers steal Wyndham's clients' PII, on information and belief, the stolen names, Social Security numbers, email addresses and loan data are now for sale on the dark web—a key motivating element for hackers engaged in data breaches of this type. Hackers access and then offer for sale the stolen unencrypted, unredacted PII to other criminals. Wyndham's clients face a substantially increased risk of financial fraud for the rest of their lives.

5. The Data Breaches were a direct result of Defendant's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect clients' PII.

6. Defendant disregarded the rights of Plaintiff and Class members (defined below) by, among other things, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its systems were protected against unauthorized intrusions; failing to disclose that it did not have reasonable or adequately robust computer systems and

---

<sup>1</sup> Wyndham's *Notice of Data Incident*, dated Oct. 16, 2020, archived by the Washington State Attorney General, available at: [https://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/Supporting\\_Law\\_Enforcement/WyndhamCapitalMortgageInc.2020-10-16.pdf](https://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/Supporting_Law_Enforcement/WyndhamCapitalMortgageInc.2020-10-16.pdf) (last accessed Dec. 1, 2020).

<sup>2</sup> Wyndham's *Notice of Data Incident*, dated Oct. 23, 2020, archived by the New Hampshire State Attorney General, available at: <https://www.doj.nh.gov/consumer/security-breaches/documents/wyndham-capital-mortgage-20201023.pdf> (last accessed Dec. 1, 2020).

security practices to safeguard clients' PII; failing to take standard and reasonably available steps to prevent the Data Breaches; failing to monitor and timely detect the Data Breaches; and failing to provide Plaintiff and Class members prompt and accurate notice of the Data Breaches.

7. As a result of Defendant's failure to implement and follow reasonable security procedures, Defendant's current and former clients' PII is now in the hands of thieves. Plaintiff and Class members have had to spend, and will continue to spend, significant amounts of time and money in an effort to protect themselves from the adverse ramifications of the Data Breaches and will forever be at a heightened risk of identity theft and fraud—especially with Defendant's loss of their Social Security numbers and similar sensitive and confidential information. Plaintiff, on behalf of all others similarly situated, alleges claims for negligence, declaratory relief, unjust enrichment; breach of implied contract, breach of confidence, and violation of Florida's Deceptive and Unfair Trade Practices Act (Florida Statute § 501.203, *et seq.*). Plaintiff and the Class members seek to compel Defendant to adopt reasonably sufficient security practices to safeguard current and former clients' PII that remains in Defendant's custody to prevent incidents like the Data Breaches from reoccurring in the future.

### **PARTIES**

8. Plaintiff Ethan Darnell is a citizen of Florida residing in Baker County. Mr. Darnell applied for and received a home loan from Wyndham in or about January 2020, then refinanced the loan through Wyndham in or about June 2020. Wyndham "sold" the loan to another finance company shortly after the refinancing, before the Data Breaches. Mr. Darnell received Wyndham's *Notice of Data Breach* on or about October 16, 2020.

9. Defendant Wyndham Capital Mortgage, Inc., is a privately held North Carolina corporation, with its principle place of business located at 4064 Colony Road, Moorcroft II, Floor 2, Charlotte, North Carolina. Defendant offers home loan services to residents nationwide through referrals, advertising, and its website, wyndhamcapital.com.

10. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently

unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

11. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

### **JURISDICTION AND VENUE**

12. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class. Moreover, this Court has jurisdiction over this action under 28 U.S.C. § 1332(a)(1) because Plaintiff is a Florida citizen and therefore diverse from Defendant, which is a North Carolina citizen.

13. This Court has personal jurisdiction over Defendant because Defendant is located in North Carolina, with its principal place of business within this District.

14. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District. Defendant resides within this judicial district and substantial part of the events giving rise to the claims alleged herein occurred within this judicial district.

### **FACTUAL ALLEGATIONS**

#### ***Background***

15. Wyndham Capital Mortgage Inc. is a mortgage company that provides residential mortgage loans through direct-to-consumer, online lending. It employs robotic process automation and other AI systems "to reduce manual intervention and menial tasks in their mortgage approval processes."<sup>3</sup> The company was founded in 2003 and has mortgage consultants licensed across the nation, including California, Florida, New Jersey, and North Carolina, to name a few.

---

<sup>3</sup> *Wyndham Capital Mortgage Partners with AI Foundry For Lending AI Solutions*, AI Foundry Press Release, May 5, 2020, available at: <https://www.prnewswire.com/news-releases/wyndham-capital-mortgage-partners-with-ai-foundry-for-lending-ai-solutions-301052190.html> (last accessed Dec. 2, 2020).

16. Although Wyndham has operated primarily online since it was founded, over the last year it has become increasingly popular, with more than double the traffic since 2019.<sup>4</sup> Beginning in 2019, the company began rapidly expanding its sales and operation teams in an effort to keep up with increased demand for online mortgage services.<sup>5</sup>

17. Plaintiff and Class members applied for mortgages with Wyndham, requiring them to provide some of their most sensitive and confidential information, including names, dates of birth, financial account numbers, and Social Security numbers and other personal identifiable information which are static, do not change, and can be used to commit myriad financial crimes now or in the future.

### ***The Data Breaches***

18. Beginning on or about October 16, 2020, Wyndham sent numerous states' Attorneys General a *Notice of Data Incident*. Wyndham's outside counsel at Baker Donelson informed the Attorneys General:

This correspondence is to notify you of potential security issue caused by a recent single occurrence of user error. On September 18, 2020, an email containing personal information was sent in error to an email account not belonging to WCM. WCM has no evidence that this email was opened or that the information has been used. Upon identifying the incident, WCM immediately took action to address the problem, including an attempted recall of the email and attempted communications to the mailbox owner and service provider to have the email deleted. WCM has put additional protections in place to keep this from happening again, has provided additional training to employees, and continues to strengthen system controls and monitoring.

[. . .] The personally identifiable information ("PII") that was potentially at risk included

---

<sup>4</sup> Wyndham Capital CEO Jeff Douglas Named a HousingWire Tech Trendsetter Award Winner, available at: <https://www.wyndhamcapital.com/blog/wyndham-capital-ceo-jeff-douglas-named-a-housingwire-tech-trendsetter-award-winner> (last accessed Dec. 1, 2020).

<sup>5</sup> Wyndham Capital Mortgage Expands Nationally and Locally, Launches New Model to Meet Loan Officer Needs, Wyndham Press Release, Nov. 21, 2019, available at: <https://www.prnewswire.com/news-releases/wyndham-capital-mortgage-expands-nationally-and-locally-launches-new-model-to-meet-loan-officer-needs-300962724.html#:~:text=Wyndham%20Capital%20Mortgage%20Inc&text=In%20addition%20to%20growing%20nationally,its%20headquarters%20in%20early%202020.&text=The%20new%20headquarters%20will%20be,want%20to%20come%20to%20work> (last accessed Dec. 2, 2020).

names, email addresses, Social Security numbers, and loan data.<sup>6</sup>

19. A week later, on or about October 23, 2020, Wyndham's counsel sent the Attorneys General another Notice of Data Incident, stating:

This correspondence is to notify you of potential security issue caused by a phishing scam. WCM discovered that an employee was the victim of a phishing scam which allowed access to the employee's email account for a limited period of time. Upon discovery, WCM took immediate action; WCM blocked the unauthorized access, changed passwords and launched an investigation. In response to this incident, WCM has put additional protections in place to keep this from happening again, has provided additional training to employees, and continues to strengthen system controls and monitoring.

[. . .] The personally identifiable information ("PII") that was potentially at risk included names, email addresses, Social Security numbers, and loan data.<sup>7</sup>

20. In the sample *Notice of Data Breach* meant for Wyndham's affected clients, attached to the notice to the various Attorneys General, Wyndham elaborated on the breach:

**What Happened**

For the period of June 30, 2020 through August 3, 2020, there appears to have been a compromise to our security protocols that allowed unauthorized access to an email account for one employee. We understand it is our responsibility to protect your information.

**What Information Was Involved**

Data elements exposed may include the following:

- Name
- Social Security Number
- Date of Birth
- Credit Score

21. In the *Notice of Data Breach* attached to Wyndham's October 16, 2020 notice to the Attorneys General, Wyndham offered affected individuals one year of credit monitoring. In addition, Wyndham recommended that affected individuals "take precautions" in response to the Data Breaches, including:

---

<sup>6</sup> Wyndham's *Notice of Data Incident* dated Oct. 16, 2020, *supra* note 1.

<sup>7</sup> Wyndham's *Notice of Data Incident* dated Oct. 23, 2020, *supra* note 2.

Carefully review your credit reports, debit/credit card, insurance policy, bank account and other account statements. Activate alerts on your bank accounts to notify you of suspicious activity. Report suspicious or fraudulent charges to your insurance statements, credit report, credit card or bank accounts to your insurance company, bank/credit card vendor and law enforcement.

22. Wyndham's current and former clients' PII has been compromised by third parties and malicious actors and Plaintiff—who has not had a relationship with Wyndham for months—did not authorize the dissemination thereto.

***Plaintiff's Efforts to Secure Their PII***

23. Upon receiving Notice from Wyndham on or about October 16, 2020, Plaintiff researched his options to respond to the theft of his name, Social Security number, email address and loan data. He contacted his bank and signed up for the credit monitoring offered by Defendant. Mr. Darnell also contacted Wyndham to further enquire about the theft of his PII. He continues to spend additional time routinely reviewing his credit monitoring service results and reports. This is time Plaintiff otherwise would have spent performing other activities, such as his job and/or leisurely activities for the enjoyment of life.

24. Knowing that thieves stole his PII, including his Social Security number and other sensitive financial information, and knowing that his PII will be sold on the dark web, has caused Plaintiff great anxiety.

25. Plaintiff has not been involved in any other data breaches, and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. He deletes any and all electronic documents containing PII, and destroys any documents that contain any of his PII, or that may contain any information that could otherwise be used to compromise his PII.

26. Plaintiff suffered actual injury from having his PII exposed as a result of the Data Breaches including, but not limited to: (a) damages to and diminution in the value of his PII—a form of intangible property that the Plaintiff entrusted to Wyndham as a condition of his employment; (b) loss of his privacy; and (c) imminent and impending injury arising from the

increased risk of fraud and identity theft.

27. As a result of the Data Breaches, Plaintiff will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

***Wyndham Acquires, Collects and Stores Plaintiff's and Class members' PII.***

28. Wyndham acquires, collects, and stores its clients' PII.<sup>8</sup>

29. As a condition of applying for a mortgage with Wyndham, Wyndham requires that its applicants entrust it with highly confidential PII.

30. By obtaining, collecting, and storing Plaintiff's and Class members' PII, Wyndham assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class members' PII from disclosure.

31. In Wyndham's Privacy Policies, Wyndham includes an exhaustive list of "Reasons we can share your personal information"; none of which include allowing criminals to exfiltrated unencrypted personal information belonging to current or former clients.

32. Moreover, Wyndham states: "To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."

33. Plaintiff and the Class members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and the Class Members, as current and former clients, relied on Wyndham to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

***The Value of PII and the Effects of Unauthorized Disclosure.***

34. Wyndham was well aware that the PII it collects, stores, and maintains is highly sensitive and of significant value to those who would use it for wrongful purposes.

35. The PII of consumers remains of high value to criminals, as evidenced by the

---

<sup>8</sup> Wyndham's *Privacy Policy*, available at: <https://www.wyndhamcapital.com/privacy-policy> (last accessed Dec. 1, 2020).

prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.<sup>9</sup> Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.<sup>10</sup> Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.<sup>11</sup>

36. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.<sup>12</sup>

37. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

---

<sup>9</sup> *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed Dec. 2, 2020).

<sup>10</sup> *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last accessed Dec. 2, 2020).

<sup>11</sup> *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed Dec. 2, 2020).

<sup>12</sup> Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Dec. 2, 2020).

38. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, “The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”<sup>13</sup>

39. Based on the foregoing, the information compromised in the Data Breaches is significantly more valuable than the loss of, for example, only credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in the Data Breaches is impossible to “close” and difficult, if not impossible, to change—Social Security number, name, date of birth, and addresses and possible other information included in Wyndham’s vague definition of “loan data.”

40. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”<sup>14</sup>

41. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

42. The fraudulent activity resulting from the Data Breaches may not come to light for years.

43. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data

---

<sup>13</sup> Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft> (last visited Dec. 2, 2020).

<sup>14</sup> Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Dec. 2, 2020).

may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.<sup>15</sup>

44. At all relevant times, Wyndham knew, or reasonably should have known, of the importance of safeguarding its current and former clients' PII, including Social Security numbers dates of birth, and "loan data," and of the foreseeable consequences that would occur if Wyndham's data security system was breached, including, specifically, the significant costs that would be imposed on Wyndham's current and former clients as a result of a breach.

45. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

46. Wyndham was, or should have been, fully aware of the unique type and the significant volume of data it collected, amounting to thousands of individuals' detailed PII and thus, the significant number of individuals who would be harmed by Wyndham's loss of that unencrypted data.

47. The injuries to Plaintiff and Class members were directly and proximately caused by Wyndham's failure to implement or maintain adequate data security measures for its current and former clients' PII.

***Wyndham Failed to Comply with FTC Guidelines.***

48. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.<sup>16</sup>

---

<sup>15</sup> *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <http://www.gao.gov/new.items/d07737.pdf> (last visited Dec. 2, 2020).

<sup>16</sup> Federal Trade Commission, *Start With Security*, available at: <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last accessed Dec. 2, 2020).

49. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.<sup>17</sup> The guidelines note that **businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement policies to correct any security problems.**

50. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.<sup>18</sup>

51. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect personal data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential personal data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

52. Wyndham failed to properly implement basic data security practices. Wyndham’s failure to employ reasonable and appropriate measures to protect against unauthorized access to current and former clients’ PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

53. Wyndham was at all times fully aware of its obligation to protect the PII of current and former employees because of its position as a trusted employer. Wyndham was also aware of the significant repercussions that would result from its failure to do so.

---

<sup>17</sup> Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last accessed Dec. 2, 2020).

<sup>18</sup> FTC, *Start With Security*, *supra* note 15.

***Plaintiff and Class Members Suffered Damages.***

54. The ramifications of Defendant's failure to keep current and former clients' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.<sup>19</sup>

55. The PII belonging to Plaintiff and Class members is private, sensitive in nature, and was left inadequately protected by Defendant who did not obtain Plaintiff's or Class members' consent to disclose such PII to any other person as required by applicable law and industry standards.

56. The Data Breaches were a direct and proximate result of Wyndham's failure to: (a) properly safeguard and protect Plaintiff's and Class members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' PII; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

57. Wyndham had the resources necessary to prevent the Data Breaches, but neglected to adequately implement data security measures, despite its obligation to protect current and former clients' PII.

58. Had Wyndham adopted security measures recommended by experts in the field, it would have prevented the intrusions into its systems and, ultimately, the theft of PII.

59. As a direct and proximate result of Wyndham's wrongful actions and inactions, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breaches on their lives.

---

<sup>19</sup> 2014 LexisNexis True Cost of Fraud Study, available at: <https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf> (last accessed Dec. 2, 2020).

60. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."<sup>20</sup>

61. As a result of the Wyndham's failures to prevent the Data Breach, Plaintiff and Class members have suffered, will suffer, and are at increased risk of suffering:

- a. The compromise, publication, theft, and/or unauthorized use of their PII;
- b. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;
- c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breaches, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;
- d. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Wyndham fails to undertake appropriate measures to protect the PII in its possession; and
- e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breaches for the remainder of the lives of Plaintiff and Class members.

62. In addition to a remedy for the economic harm, Plaintiff and the Class members maintain an undeniable interest in ensuring that their PII is secure, remains secure, and is not subject to further misappropriation and theft.

---

<sup>20</sup> U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft*, 2012, December 2013, available at: <https://www.bjs.gov/content/pub/pdf/vit12.pdf> (last accessed Dec. 2, 2020).

### **CLASS ALLEGATIONS**

63. Plaintiff bring this nationwide class action pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following class:

All individuals whose PII was compromised in the Data Breaches announced by Wyndham in October 2020 (the “Nationwide Class”).

64. The Florida Subclass is defined as follows:

All persons residing in Florida whose PII was compromised in the Data Breaches announced by Wyndham in October 2020 (the “Florida Subclass”).

65. Excluded from the Class are the following individuals and/or entities: Defendant and its parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Defendant have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to Defendant’s departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as Defendant’s immediate family members.

66. Plaintiff reserve the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

67. **Numerosity:** The Classes are so numerous that joinder of all members is impracticable. Defendant has identified thousands of customers whose PII may have been improperly accessed in the Data Breaches, and the Classes are apparently identifiable within Defendant’s records.

68. **Commonality:** Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class members. These include:

- a. When Defendant actually learned of the data breaches and whether their response was adequate;
- b. Whether Defendant owed a duty to Plaintiff and the Class to exercise due care in

collecting, storing, safeguarding and/or obtaining their PII;

- c. Whether Defendant breached that duty;
- d. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiff's and Class members' PII;
- e. Whether Defendant acted negligently in connection with the monitoring and/or protection of Plaintiff's and Class members' PII;
- f. Whether Defendant knew or should have known that they did not employ reasonable measures to keep Plaintiff's and Class members' PII secure and prevent loss or misuse of that PII;
- g. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breaches to occur;
- h. Whether Defendant caused Plaintiff and Class members damages;
- i. Whether Defendant violated the law by failing to promptly notify Class members that their PII had been compromised;
- j. Whether Plaintiff and the other Class members are entitled to credit monitoring and other monetary relief;
- k. Whether Defendant violated Florida's Deceptive and Unfair Trade Practices Act (Florida Statute § 501.203, *et seq.*); and

69. **Typicality:** Plaintiff's claims are typical of those of other Class members because all had their PII compromised as a result of the Data Breaches, due to Defendant's misfeasance.

70. **Adequacy:** Plaintiff will fairly and adequately represent and protect the interests of the Class members. Plaintiff's Counsel are competent and experienced in litigating privacy-related class actions.

71. **Superiority and Manageability:** Under 23(b)(3), a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Individual damages for any individual Class member are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class

treatment, Defendant's misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

72. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2) because Defendant have acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

73. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendant owed a legal duty to Plaintiff and Class members to exercise due care in collecting, storing, using, and safeguarding their PII;
- b. Whether Defendant breached a legal duty to Plaintiff and the Class members to exercise due care in collecting, storing, using, and safeguarding their PII;
- c. Whether Defendant failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;
- d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breaches; and
- e. Whether Class members are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

### **FIRST CLAIM FOR RELIEF**

#### **Negligence**

#### **(On Behalf of Plaintiff and the Nationwide Class)**

74. Plaintiff re-alleges and incorporate by reference herein all of the allegations contained in paragraphs 1 through 73.

75. Defendant owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, using, and protecting their PII from unauthorized third parties.

76. The legal duties owed by Defendant to Plaintiff and Class members include, but are not limited to the following:

- a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of Plaintiff and Class members in their possession;
- b. To protect PII of Plaintiff and Class members in their possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and
- c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiff and Class members of the data breach.

77. Defendant's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45(a), which prohibits "unfair . . . practices in or affecting commerce," including, as interested and enforced by the FTC, the unfair practices of failing to use reasonable measures to protect PII by companies such as Defendant.

78. Various FTC publications and data security breach orders further form the basis of Defendant's duty. Plaintiff and Class members are consumers under the FTC Act. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with industry standards.

79. Defendant breached its duties to Plaintiff and Class members. Defendant knew or should have known the risks of collecting and storing PII and the importance of maintaining secure systems, especially in light of the facts that hacks of this nature increase every year.

80. Defendant knew or should have known that its security practices did not adequately safeguard Plaintiff's and Class members' PII, including, but not limited to, the failure to properly train employees regarding phishing scams and failure to detect the unauthorized third parties'

access to Wyndham's employee's email account for an extensive period; from June 30, 2020 through August 3, 2020.

81. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and their failure to protect the PII of Plaintiff and the Class from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, accessed, and misused, Defendant unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiff's and Class members' PII during the period it was within Defendant's possession and control.

82. Defendant breached the duties they owe to Plaintiff and Class members in several ways, including:

- a. Failing to implement adequate security systems, protocols, and practices sufficient to protect customers' PII and thereby creating a foreseeable risk of harm;
- b. Failing to comply with the minimum industry data security standards during the period of the data breach;
- c. Failing to act despite knowing or having reason to know that Defendant's systems were vulnerable to phishing or similar attacks (*e.g.*, Defendant did not detect the unauthorized third parties' access to the email account for months, nor did they implement safeguards in light of the surge of similar attacks in the online community); and
- d. Failing to timely and accurately disclose to customers that their PII had been improperly acquired or accessed and was potentially available for sale to criminals on the dark web.

83. Due to Defendant's conduct, Plaintiff and Class members are entitled to credit monitoring. Credit monitoring is reasonable here. The PII taken can be used towards identity theft and other types of financial fraud against the Class members. Hackers not only stole many of Wyndham's current and former clients' names from the website, they also stole clients' "loan data," email addresses and Social Security numbers. They got everything they need to illegally

adopt Wyndham's clients' identities, and to abuse those clients' financial accounts to make illegal purchases. There is no question that this PII was taken by sophisticated cybercriminals, increasing the risks to the Class members. The consequences of identity theft are serious and long-lasting. There is a benefit to early detection and monitoring.

84. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach. Annual subscriptions for credit monitoring plans range from approximately \$219 to \$358 per year.

85. As a result of Defendant's negligence, Plaintiff and Class members suffered injuries that may include: (i) the lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from financial fraud and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the data breach, including but not limited to time spent deleting phishing email messages and cancelling credit cards believed to be associated with the compromised account; (iv) the continued risk to their PII, which may remain for sale on the dark web and is in Defendant's possession, subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PII of customers and former customers in their continued possession; (v) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the PII compromised as a result of the data breach for the remainder of the lives of Plaintiff and Class members, including ongoing credit monitoring.

86. These injuries were reasonably foreseeable given the history of security breaches of this nature. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Defendant's negligent conduct.

**SECOND CLAIM FOR RELIEF**  
**Declaratory Judgment**  
**(On Behalf of Plaintiff and the Nationwide Class)**

87. Plaintiff re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 73.

88. Defendant owe duties of care to Plaintiff and Class members which would require it to adequately secure PII.

89. Defendant still possesses PII regarding Plaintiff and Class members.

90. Although Wyndham claims in their *Notice of Data Breach* that it took certain technical precautions to prevent this type of incident from occurring again, there is no detail on what, if any, fixes have really occurred.

91. Plaintiff and Class members are at risk of harm due to the exposure of their PII and Defendant's failure to address the security failings that lead to such exposure.

92. There is no reason to believe that Defendant's security measures are any more adequate than they were before the breach to meet Defendant's contractual obligations and legal duties, and there is no reason to think Defendant have no other security vulnerabilities that have not yet been knowingly exploited.

93. Plaintiff, therefore, seeks a declaration that (1) each of Defendant's existing security measures do not comply with their explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' personal information, and (2) to comply with their explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

- a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- b. Engaging third-party security auditors and internal personnel to run automated security monitoring;
- c. Auditing, testing, and training their security personnel regarding any new or modified procedures;

- d. Segmenting their consumer applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;
- e. Conducting regular database scanning and securing checks;
- f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- g. Purchasing credit monitoring services for Plaintiff and Class members for a period of ten years; and
- h. Meaningfully educating their clients about the threats they face as a result of the loss of their PII to third parties, as well as the steps Defendant's customers must take to protect themselves.

### **THIRD CLAIM FOR RELIEF**

**Violation of Florida's Deceptive and Unfair Trade Practices Act, Florida Statute § 501.203, *et seq.***

**(On Behalf of Plaintiff and the Nationwide Class, or, in the alternative, On Behalf of Plaintiff Darnell and the Florida Subclass)**

94. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 73.

95. Plaintiff and the Florida Subclass members are "consumers." Fla. Stat. § 501.203(7).

96. Plaintiff and the Florida Subclass members purchased "things of value" insofar as products and services from Defendant. These purchases were made primarily for personal, family, or household purposes. Fla. Stat. § 501.203(9).

97. Defendant engaged in the conduct alleged in this Complaint by advertising and entering into transactions intended to result, and which did result, in the sale, rental of goods, services, and/or property to consumers, including Plaintiff and the Florida Subclass members. Fla. Stat. § 501.203(8).

98. Defendant engaged in, and their acts and omissions affected trade and commerce. Defendant's acts, practices, and omissions were done in the course of Defendant's business of advertising, marketing, offering to sell, and selling and/or renting goods and services throughout Florida and the United States. Fla. Stat. § 501.203(8).

99. Defendant, operating in Florida and elsewhere through their worldwide website, engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Fla. Stat. § 501.204(1), including but not limited to the following:

- a. charging a premium for the goods and services, implicitly representing that the premium would be used to protect Plaintiff's and Florida SubClass members' protected health information and other PII;
- b. continued acceptance of credit and debit card payments and storage of other PII after Defendant knew or should have known of the Data Breaches and before they allegedly remediated the Data Breach.

100. This conduct is considered unfair methods of competition, and constitutes unfair and unconscionable acts and practices. Fla. Stat. § 501.204(1).

101. As a direct and proximate result of Defendant's violation of Florida's Deceptive and Unfair Trade Practices Act ("FDUTPA"), Plaintiff and the Florida Subclass members suffered actual damages by paying a premium for Defendant's goods and services with the understanding that at least part of the premium would be applied toward sufficient and adequate information security practices that comply with industry standards, when in fact no portion of that premium was applied toward sufficient and adequate information security practices. Fla. Stat. § 501.211(2).

102. Moreover, as a direct result of Defendant's knowing violation of FDUTPA, Plaintiff Darnell and the Florida Subclass members are not only entitled to actual damages, but also declaratory judgment that Defendant's actions and practices alleged herein violate FDUTPA, and injunctive relief, including, but not limited to:

- a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks,

penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

- b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;
- c. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;
- d. Ordering that Defendant segment PII by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;
- e. Ordering that Defendant purge, delete, and destroy in a reasonable secure manner PII not necessary for their provisions of services;
- f. Ordering that Defendant conduct regular database scanning and securing checks;
- g. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and
- h. Ordering Defendant to meaningfully educate their customers about the threats they face as a result of the loss of their financial and personal information to third-parties, as well as the steps Defendant's customers must take to protect themselves. Fla. Stat. § 501.211(1).

103. Plaintiff brings this action on behalf of himself and the Florida Subclass members for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff and the Florida Subclass members and the public from Defendant's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable, and unlawful practices. Defendant's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

104. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff Darnell and the Florida Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

105. Defendant knew or should have known that the lack of encryption on their computer systems and data security practices were inadequate to safeguard the Florida SubClass members' PII and that the risk of a data disclosure or theft was high.

106. Defendant's actions and inactions in engaging in the unfair practices and deceptive acts described herein were negligent, knowing and willful, and/or wanton and reckless.

107. Plaintiff and the Florida Subclass members seek relief under Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201, *et seq.*, including, but not limited to, damages, injunctive relief, and attorneys' fees and costs, and any other just and proper relief.

**FORTH CLAIM FOR RELIEF**  
**Unjust Enrichment**  
**(On Behalf of Plaintiff and the Nationwide Class)**

108. Plaintiff re-alleges and incorporate by reference herein all of the allegations contained in paragraphs 1 through 73.

109. Plaintiff and Class members conferred a monetary benefit upon Defendant in the form of monies paid for goods available on Defendant's websites.

110. Defendant appreciated or had knowledge of the benefits conferred upon them by Plaintiff and Class members. Defendant also benefited from the receipt of Plaintiff's and Class members' PII, as this was used by Defendant to facilitate payment to them.

111. The monies for goods that Plaintiff and Class members paid to Defendant were to be used by Defendant, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

112. As a result of Defendant's conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their purchases made with

reasonable data privacy and security practices and procedures that Plaintiff and Class members paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

113. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class members because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

114. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class members all unlawful or inequitable proceeds received by it as a result of the conduct alleged herein.

**FIFTH CLAIM FOR RELIEF**  
**Breach of Implied Contract**  
**(On Behalf of Plaintiff and the Nationwide Class)**

115. Plaintiff re-alleges and incorporate by reference herein all of the allegations contained in paragraphs 1 through 73.

116. Plaintiff and Class members were required to provide their PII, including their names, Social Security numbers, dates of birth, and sensitive and confidential information to Defendant as a condition of their applying for a residential mortgage with Defendant.

117. Plaintiff and Class members were required to provide their PII when they applied for a mortgage with Defendant, and implied in that exchange of information was Defendant's promise to protect their PII from unauthorized disclosure.

118. Further implicit in this agreement between Plaintiff and Class members and the Defendant was Defendant's obligation to: (a) use such PII for business purposes only; (b) take reasonable steps to safeguard that PII; (c) prevent unauthorized disclosures of the PII; (d) provide Plaintiff and Class members with prompt and sufficient notice of any and all unauthorized access

and/or theft of their PII; and (e) retain the PII only under conditions that kept such information secure and confidential.

119. Without such implied contracts, Plaintiff and Class members would not have provided their PII to and applied for residential mortgages with Defendant.

120. Plaintiff and Class members fully performed their obligations under the implied contract with Defendant, however, Defendant did not.

121. Defendant breached the implied contracts with Plaintiff and Class members by failing to reasonably safeguard and protect Plaintiff's and Class members' PII, which was compromised as a result of the Data Breaches.

122. As a direct and proximate result of Wyndham's breach of the implied contracts, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from the Data Breaches including, but not limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession; and (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breaches for the remainder of the lives of Plaintiff and Class Members.

**SIXTH CLAIM FOR RELIEF**  
**Breach of Confidence**  
**(On Behalf of Plaintiff and the Nationwide Class)**

123. Plaintiff re-alleges and incorporate by reference herein all of the allegations contained in paragraphs 1 through 73.

124. At all times during Plaintiff's and Class members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class members' PII that Plaintiff and Class members provided to Defendant.

125. As alleged herein and above, Defendant's relationship with Plaintiff and Class members was governed by terms and expectations that Plaintiff's and Class members' PII would be collected, stored, and protected in confidence, and would not be disclosed the unauthorized third parties.

126. Plaintiff and Class members provided their respective PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to unauthorized parties.

127. Defendant voluntarily received in confidence Plaintiff's and Class members' PII with the understanding that the PII would not be disclosed or disseminated to the public or any unauthorized third parties.

128. Due to Defendant's failure to prevent, detect, and avoid the Data Breaches from occurring by, *inter alia*, following best information security practices to secure Plaintiff's and Class members' PII, Plaintiff's and Class members' PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class members' confidence, and without their express permission.

129. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class Members have suffered damages.

130. But for Defendant's disclosure of Plaintiff's and Class members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breaches were the direct and legal cause of the theft of Plaintiff's and Class members' PII, as well as the resulting damages.

131. The injury and harm Plaintiff and Class members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class members' PII.

Defendant knew its computer systems and technologies for accepting and securing Plaintiff's and Class members' PII had numerous security and other vulnerabilities that placed Plaintiff's and Class members' PII in jeopardy.

132. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession; and (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breaches for the remainder of the lives of Plaintiff and Class Members.

### **PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiff, on behalf of himself and all Class members, requests judgment against Defendant and that the Court grant the following:

- A. An order certifying the Nationwide Class and Florida Subclass, as defined herein, and appointing Plaintiff and his counsel to represent the classes;
- B. An order enjoining Defendant from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of Plaintiff's and Class members' PII;
- C. An order instructing Defendant to purchase or provide funds for credit monitoring services for Plaintiff and all Class members;
- D. An award of compensatory, statutory, nominal and punitive damages, in an amount to be determined at trial;

- E. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;
- F. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and
- G. Such other and further relief as this Court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiff hereby demands that this matter be tried before a jury.

Date: December 10, 2020

Respectfully Submitted,

By: /s/ Jean S. Martin  
JEAN MARTIN  
JOHN A. YANCHUNIS  
*(Pro Hac Vice application forthcoming)*  
RYAN J. MCGEE  
*(Pro Hac Vice application forthcoming)*  
**MORGAN & MORGAN**  
201 N. Franklin Street, 7th Floor  
Tampa, Florida 33602  
(813) 223-5505  
[jyanchunis@ForThePeople.com](mailto:jyanchunis@ForThePeople.com)  
[jeanmartin@ForThePeople.com](mailto:jeanmartin@ForThePeople.com)  
[rmcgee@ForThePeople.com](mailto:rmcgee@ForThePeople.com)

M. ANDERSON BERRY  
*(Pro Hac Vice application forthcoming)*  
LESLIE GUILLON  
*(Pro Hac Vice application forthcoming)*  
**CLAYEO C. ARNOLD,**  
**A PROFESSIONAL LAW CORP.**  
865 Howe Avenue  
Sacramento, CA 95825  
(916) 777-7777  
[aberry@justice4you.com](mailto:aberry@justice4you.com)  
[lguillon@justice4you.com](mailto:lguillon@justice4you.com)